Московский Физико-Технический Институт
(государственный университет)

Факультет общей и прикладной физики
Проблемы "Проблемы теоретической физики"

Дипломная работа

студента 928 группы Баяндина К.В.

Использование запутанных квантовых состояний для передачи зашифрованных сообщений.

Научный руководитель:
д.ф.м.н. Лесовик Б.Г.

Москва
2003

Содержание

Введение

Двадцатый век принчс криптоаналитикам систему кодирования RSA [1], которая сегодня широко используется. Эта система шифрования позволяет решить многие криптографические задачи и реализовать различные протоколы. Этот метод шифрования использует свойства простых чисел и теоремы алгебры. Общеизвестно, что он использует одностороннюю функцию, которая легко вычисляется, но обратить еч можно, лишь зная секретный ключ, без которого задача обращения этой функции получится очень сложной. Секретный ключ в данном случае - это разложение на простые делители большого числа, которое общеизвестно. Вся система шифрования основана на убеждении, что не существует полиномиального алгоритма разложения числа на простые делители. Поэтому обладатель секретного ключа может не опасаться, что кто-нибудь другой в обозримом будущем узнает разложение этого числа на простые множители.

Но оказывается, что не всч так безоблачно, как казалось раньше. Ещч в восьмидесятых годах Фейнман высказал догадку [2], что вычислительная машина построенная на законах квантовой механики способна решать задачи быстрее, чем любая классическая. Совсем недавно Шор предложил свой, уже ставший знаменитым, квантовый алгоритм разложения большого числа на простые делители [3], который решает задачу за полиномиальное время от размера числа.

В последнее время были созданы квантовые компьютеры работающие с несколькими кубитами. И хотя создание систем с тысячами кубитов, необходимых для алгоритма Шора, ещч дело очень отдалчнного будущего, всч равно, сама возможность их создания отбрасывает тень на систему шифрования RSA. Неудивительно, что уже сейчас ведутся обширные исследования в этой области.

Самое интересное, что квантовые компьютеры не только разрушат популярную криптографическую схему, но они так же откроют новый путь шифрования информации.

Уже сейчас предложены и реализованы способы передачи сообщений, существенным образом использующие законы квантовой механики. В данной работе сначала кратко будут разобраны два протокола получения секретного ключа, которые непосредственно используют законы квантовой механики. Потом будет предложен вариант передачи сообщений, зашифрованных при помощи запутанных состояний спинов.

1 Квантовое разделение секретного ключа.

1.1 Постановка задачи получения ключа

Для удобства будем в дальнейшем называть отправителя секретного сообщения Алисой, а получателя - Бобом. Естественно, что когда-нибудь объявиться взломщик, который захочет подслушивать их переговоры, его мы будем называть Евой. Мы будем считать, что возможности Евы ограниченны лишь современными технологиями, Алиса и Боб знают это, и поэтому стараются передавать свои сообщения с расччтом, что при всех своих возможностях Ева сможет их расшифровать лишь через несколько лет.

Согласно теории информации Шеннона [4], любой долгоиспользуемый метод шифрования уязвим, и у взломщика всегда существует некоторая, хоть и очень малая, вероятность разгадать шифр. Единственным абсолютно защищчнным способом передачи информации является следующий: Алиса, переведя всю имеющуюся у неч информацию в последовательность битов, применяет к ним операцию "исключающего или" вместе с последовательностью битов случайного ключа, который был создан когда-либо в прошлом при личной встрече с Бобом. Длина секретного ключа должна быть не меньше длины передаваемого сообщения, и ключ должен использоваться строго один раз. Неудобством такого способа является то, что в любом случае Алисе и Бобу необходимо хранить огромное количество ключей, а в случае, если кому-либо из них придчтся общаться с третьим партнчром, то и для него придчтся хранить множество ключей, что очевидно очень неудобно.

Ниже приведены два способа позволяющие надчжно получить секретный случайный ключ находясь на удалении друг от друга. Надчжность такой системы определяется тем, с какой вероятностью Алиса и Боб могут позволить рассекречивание шифра.

1.2 Посылка неортогональных состояний

Квантовое распределение ключа с поляризованными состояниями впервые было предложено Ч. Х. Беннетом и Г. Брассаром [5], им при помощи импульсов зелчного света удалось произвести данную процедуру на расстоянии 40 см. Первое практическое воплощение этого метода было осуществлено в университете Женевы [6]

Кратко суть метода состоит в следующем. Алиса посылает Бобу фотоны с различными состояниями поляризации. Приччм Алиса может выбирать случайным образом направление ортов базиса - обычно два направления под углом 45 градусов друг другу, а так же она может выбирать, опять же случайно, вдоль или перпендикулярно выбранному направлению она будет поляризовать посылаемый фотон. Боб, получая фотоны от Алисы, измеряет их состояния в двух базисах, выбирая базис случайным образом. После того, как Боб измерил состояния фотонов, он по открытому каналу связи сообщает, по номерам, какие фотоны он измерял в каких базисах. После этого Алиса, опять же по открытому каналу сообщает Бобу, какие из фотонов были измерены в правильном базисе.

Теперь, в совпавших базисах, Алиса знает поляризацию каждого из фотонов, которые она посылала, а Боб все их измерил в правильном базисе, таким образом они оба обладают некоторой случайной последовательностью битов. Приччм они могут проверить, а действительно ли у них одинаковые ключи, для этого один из них может разгласить часть из полученных им битов, чтобы второй мог проверить, совпадают ли они с его битами.

Возникает вопрос, а может ли каким либо образом Ева тоже узнать эту последовательность битов? Естественно, что она может перехватывать фотоны и посылать что-нибудь Бобу. Но тут в игру вступает квантовая механика. Так как до конца передачи фотонов Алисой Ева не знает, в каких базисах они посылались, то она, во-первых, не может корректно измерить состояния фотонов, а, во-вторых, она, в силу теоремы о невозможности клонирования квантово-механической системы [7], не может

послать Бобу точно такой же фотон, оставив себе копию на будущее.

В научной литературе рассмотрены различные стратегии действий Евы. Она может измерять фотон Алисы в произвольном базисе и посылать Бобу тот, фотон, который у неч получиться после измерения. Либо она может сохранять каким-либо образом фотоны, а в сообщениях Бобу вести себя как Алиса, и после разглашения Бобом и Алисой своих базисов, она сможет корректно измерить состояния фотонов Алисы, и узнать, какой секретный ключ получился у Алисы, а какой у Боба. Но уже показано, что при любых действиях Евы, Алиса и Боб с вероятностью почти единица определят, что она им мешала.

1.3 Обмен запутанными фотонами

В этом методе Алиса получает пару фотонов, поляризации которых образуют запутанное состояние вида

$$|\Psi\rangle = \frac{1}{\sqrt{2}} \left(|\uparrow\rangle |\downarrow\rangle \ - |\downarrow\rangle \| \uparrow\rangle \right), \tag{1}$$

где стрелочки символизируют различные ортогональные состояния поляризации фотона.

Дальше Алиса и Боб, например, могут действовать следующим образом. Алиса измеряет свой фотон в базисах повчрнутых относительно исходного на углы

$$\varphi_1^a = 0, \tag{2}$$

$$\varphi_2^a = \frac{\pi}{4}, \tag{3}$$

$$\varphi_3^a = \frac{\pi}{8}. \tag{4}$$

А Боб - в базисе повчрнутом на углы

$$\varphi_1^b = 0, \tag{5}$$

$$\varphi_2^b = -\frac{\pi}{8}, \tag{6}$$

$$\varphi_3^b = \frac{\pi}{8}. \tag{7}$$

После этого Алиса и Боб разглашают при помощи открытых каналов связи, в каких базисах они измеряли каждый фотон. В случае выбора одинаковых базисов их результаты будут в точности антискоррелированны, что дачт возможность получить один бит ключа.

Теперь необходимо пояснить, каким образом Алиса и Боб могут узнать, вмешивалась ли Ева в их переговоры. Для этого они разглашают результаты измерений состояний фотонов, базисы которых были выбраны по-разному. А затем по этим данным можно посчитать величину

$$S = E\left(\varphi_1^a, \varphi_3^b\right) + E\left(\varphi_1^a, \varphi_2^b\right) + E\left(\varphi_2^a, \varphi_3^b\right) - E\left(\varphi_2^a, \varphi_2^b\right), \tag{8}$$

где

$$E\left(\varphi_i^a, \varphi_j^b\right) = P_{++}\left(\varphi_i^a, \varphi_j^b\right) + P_{--}\left(\varphi_i^a, \varphi_j^b\right) - P_{+-}\left(\varphi_i^a, \varphi_j^b\right) - P_{-+}\left(\varphi_i^a, \varphi_j^b\right), \tag{9}$$

а $P_{\pm\pm}\left(\varphi_i^a, \varphi_j^b\right)$ в свою очередь означает вероятность того, что в базисе Алисы, определяемым углом φ_i^a, был получен результат ± 1, и в базисе Боба, определяемым углом φ_j^b, был получен результат ± 1, здесь $+1$ или -1 означает две различные ортогональные ориентации поляризации фотона.

Согласно законам квантовой механики

$$P_{\pm\pm}\left(\varphi_i^a, \varphi_j^b\right) = \frac{1}{2}\left(\frac{1 + (\pm 1)(\pm 1)\cos\left(2(\varphi_i^a - \varphi_j^b)\right)}{2}\right). \tag{10}$$

Тогда

$$E\left(\varphi_i^a, \varphi_j^b\right) = -\cos\left(2(\varphi_i^a - \varphi_j^b)\right). \tag{11}$$

Согласно (2)-(7) и (11) для (8) должно получаться

$$S = -2\sqrt{2}. \tag{12}$$

Теперь осталось лишь заметить, что Ева не может получить никакой информации о результатах, получаемых при измерениях Алисой и Бобом, не возмущая запутанного состояния этих двух частиц, но такие действия согласно обобщчнной теореме Белла [8], предложенной Клаузером, Хорном, Шимони и Хольтом, приведут к уменьшению модуля S, а это сразу же можно будет заметить.

2 Передача сообщений при помощи запутанных состояний.

2.1 Постановка задачи

В дальнейшем мы будем рассматривать другую схему передачи сообщений. Основная идея этой схемы заключается в том, чтобы кодировать различные наборы битов информации запутанными состояниями достаточно большого набора спинов. Тогда основное утверждение, которое гарантирует нам защищчнность информации, заключается в том, что, не зная структуры запутанных состояний, невозможно за одно измерение в вероятностью близкой к единице определить, какое это было состояние. Во всчм последующем изложении мы будем изучать, какое количество времени понадобиться Еве, чтобы определить структуру передаваемых запутанных состояний.

Первым делом должен возникнуть вопрос, зачем этим заниматься, если можно гораздо проще, на тех же принципах, получать секретные ключи, а потом ими пользоваться. Можно привести несколько аргументов: во-первых, для протоколов обмена ключами необходимо несколько пересылок информации туда и обратно, а в случае удалчнных пользователей может быть критическим время передачи сообщения, во-вторых, такого рода "квантовая связь" может быть полезной при соединении в вычислительные "квантовые сети" нескольких будущих квантовых компьютеров, ну, и,

в-третьих, довольно полезным само по себе может оказаться изучение самой структуры запутанных состояний, а так же способов их получения.

Итак, Алиса, чтобы передать некоторую информацию Бобу, разбивает еҷ на слова по K битов. Затем она приготавливает состояние K битов с определҷнными значениями проекций относительно некоторой выбранной оси, одно из направлений задаҷт единицу, а второе ноль. После, она "зашифровывает" информацию, применяя к каждому слову при помощи квантового компьютера некоторое унитарное преобразование U, получая тем самым запутанные состояния, которые и посылает Бобу. Получатель запутанных состояний проводит над ними обратное унитарное состояние U^{-1}, получая набор спинов в чистых состояния, которые могут быть промерены с единичной вероятностью.

Естественно, есть Ева, которая хочет перехватить и расшифровать сообщение. Конечно же, она не знает секретного унитарного преобразования, используемого Алисой и Бобом. Если Ева подслушает сообщение, то есть перехватит посылаемые спины, и попытается провести над ними измерение, то она не только разрушит запутанное состояние, но получит так же результат, который имеет вероятностную природу.

Наша дальнейшая задача состоит в том, чтобы оценить количество измерений необходимое для того, чтобы Ева смогла разгадать унитарное преобразование, или что тоже самое научиться измерять перехватываемые сообщения с вероятностью близкой к единице. Опираясь на эти вычисления Алиса и Боб будут выбирать количество спинов K в сообщении и "безопасное" время использования унитарного преобразования.

Теперь необхоимо обговорить способы, при помощи которых Ева вообще может определить сектретное унитарное преобразование. В этом вопросе нужно принимать во внимание, что Ева может обладать некоторой априорной информацией, например, о временных корреляциях в появлении сообщений, или она иногда просто может знать, что за информация передаҷтся по каналу связи.

Будем различать два типа задачи: в первом Ева точно знает, какие из переданных запутанных состояний соответствуют одним и тем же сообщениям, а во втором - Ева знает лишь временные корреляции в появлении сообщений. Вторая постановка задачи значительно сложнее, поэтому еҷ решение будет рассказано в виде идеи.

2.2 Состояния, операторы и квантовые вентили

Чтобы дальше говорить о состояниях, мы должны точно определить, что это такое. Самый очевидный способ - это представлять каждое состояние как линейную суперпозицию состояний с определҷнными проекциями спинов вдоль выбранной оси

$$|State\rangle = C_0|00..00\rangle + C_1|00..01\rangle + C_{2^N-1}|11..11\rangle, \tag{13}$$

где C_i - комплексные числа, а нули и единички обозначают направления спина против или вдоль выбранной оси, которую мы обозначим за ось Z. Иногда будет удобнее и короче обозначать состояние целым числом равным двоичной записи из нулей и единичек, например

$$|13\rangle = |00001101\rangle. \tag{14}$$

Полезно упомянуть, что если кто-нибудь будет проводить простое измерение всех спинов вдоль оси Z, то он получит состояние $|i\rangle$ с вероятностью $|C_i|^2$, но это вовсе не

значит, что мы можем заменить все коэффициенты на действительные числа. Скоро мы увидим, какую роль играют относительные комплексные фазы для запутанных состояний.

Легко видеть, что каждое начальное состояние, приготовленное Алисой, это одно из базисных состояний $|i\rangle$, и его запись в виде столбца, имеющего одну единицу и $2^N - 1$ нулей. После унитарного сотояния получается некоторый столбец комплексных чисел. Очевидно, что унитарное преобразование задачтся матрицей получающейся при собирании вместе всех столбцов запутанных состояний.

Теперь мы можем представить любое унитарное преобразование в выбранном базисе в виде унитарной матрицы размера $2^K \times 2^K$. В частности, любое состояние будет записываться как вектор комплексных чисел - коэффициентов разложения C_i, а любое унитарное преобразование - как умножение матрицы на столбец, то есть

$$U = \begin{pmatrix} C_0^{(0)} & C_0^{(1)} & * & C_0^{(2^K-1)} \\ C_1^{(0)} & C_1^{(1)} & * & C_1^{(2^K-1)} \\ & * & * & * \\ C_{2^K-1}^{(0)} & C_{2^K-1}^{(1)} & * & C_{2^K-1}^{(2^K-1)} \end{pmatrix}, \tag{15}$$

где $C_i^{(j)}$ - i-ый коэффициент разложения j-го запутанного состояния.

Хотя работать с матрицами и столбцами очень удобно, необходимо обсудить возможные способы конструирования этих преобразований в "железе". Самый очевидный способ получать унитарные преобразования состоит в том, чтобы из простых вентилей составлять большую сеть. В последнее время придумано большое количество способов создания этих базовых вентилей, наиболее активно изучаемые их них, основаны на: полых резонаторах, линейных ионных ловушках, ядерном-магнитном резонансе, взаимодействии оптических мод в волноводах и других.

Экерт и Джоза показали [9], что любое унитарное преобразование спинов можно сколько угодно точно представить в виде сети состоящей из всевозможных однокубитовых вентилей и одного двухкубитового вентиля, например, реализующего контролируемое НЕ, которое можно записать в виде

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle, \tag{16}$$

или на языке состояний

$$\begin{array}{rcl} |00\rangle & \rightarrow & |00\rangle, \\ |01\rangle & \rightarrow & |01\rangle, \\ |10\rangle & \rightarrow & |11\rangle, \\ |11\rangle & \rightarrow & |10\rangle. \end{array} \tag{17}$$

К сожалению утверждение, что унитарное состояние можно разложить на простые кирпичики, ещч не дачт этого разложения. В довершение ко всему, на данный момент удалось реализовать квантовые сети лишь с единицами вентилей, а необходимы сотни и даже тысячи.

Но можно и до сих по не терять оптимизма. Мы не нуждаемся в полной универсальности в построении унитарных преобразований. Нам достаточно

подходящего физического объекта и возможность регулировать по желанию его гамильтониан.

В случае спинов можно взять, например, простой гамильтониан состоящий из одиночных и парных спиновых операторов

$$\hat{H} = \sum_i h_i \ \hat{\sigma}_i + \sum_{i,j} d_{ij} \ \hat{\sigma}_i \hat{\sigma}_j, \tag{18}$$

где $\hat{\sigma}_i$ - спиновые операторы, h_i - векторы задающие внешние поля, и наконец d_{ij} - матрицы описывающие парные взаимодействия спинов.

В этом случае унитарное преобразование запишется в виде

$$U(t) = e^{-\frac{i}{\hbar}\hat{H}t}. \tag{19}$$

Алиса и Боб могут выбирать унитарное преобразование, задавая время преобразования и параметры гамильтониана. Математически легко получить обратное преобразование, для этого достаточно изменить знак всех коэффициентов в гамильтониане. Физически изменить знак h_i очень просто, для этого достаточно перевернуть поле, но вот поменять знак d_{ij} весьма непростая задача. Заметим, что в случае квантовых сетей из вентилей обращение унитарного преобразования совсем не представляет сложности при известном построении прямого преобразования, так как все используемые вентили обратимы.

Представление унитарного преобразования в виде вентилей или в виде (18) и (19) - дело наглядности. Наша дальнейшая задача состоит в том, чтобы показать, что Ева должна будет потратить огромное количество времени, чтобы разгадать секретное унитарное преобразование. Именно этим мы и займчмся в дальнейшем.

3 Определение запутанного состояния.

3.1 Задачи Евы по изучению запутанных состояний

В данный момент мы начинаем обсуждение способов, при помощи которых Ева может расшифровать информацию посылаемую Алисой. Мы можем утверждать, что секретный ключ в данной системе шифрования - то унитарное преобразования. Задача Алисы - разгадать это унитарное преобразование. В этом случае у Евы есть сходные проблемы, что и в классическом случае. Общеизвестно, что кажущаяся стойкость секретного ключа может быть легко разрушена, в случае если взломщик знает априорную информацию о зашифрованных сообщениях. Например, Ева может знать частоту появления сообщений, а так же корреляции между появлениями соседних сообщений.

Случай квантовой криптографии более сложный. Ева не знает преобразования, так что еч измерения будут давать вероятностные результаты. Другими словами, она, измерив запутанное состояние, получит вероятностный ответ, по которому невозможно восстановить исходное запутанное состояние.

Для упрощения в этом разделе будем считать, что Ева либо знает, какие сообщения посылает Алиса в определчнные моменты времени, либо она точно знает,

что в определчнный отрезок времени Алиса посылает некоторое фиксированное запутанное состояние. Цель Евы будет заключаться в том, чтобы, проводя измерения этого запутанного состояния, полностью определить его. Понятно, что получив все запутанные состояния Ева сможет вывести желаемое унитарное преобразование.

Итак, в дальнейшем будем считать, что Алиса посылает одно фиксированное запутанное состояние, а Ева хочет научиться измерять его с вероятностью близкой к единице.

3.2 Определение состояния одного спина

Наиболее простой способ определять направление нескольких идентичных спинов заключается в следующем. Ева должна измерить с заданной точностью вероятности того, что спин направлен вдоль некоторой оси для двух ортогональных осей. Исходя их этих данных она может вывести направление этих спинов. В таком случае этот эксперимент сводится к определению параметра p биномиального распределения для двух различных направлений спина вдоль оси.

В самом деле вероятность того, что спин направлен под углом θ к оси Z есть

$$p = \frac{1 + \cos\theta}{2}. \tag{20}$$

Допустим, что Ева измерила спин N раз, и получила, что он n раз был направлен вдоль оси и $(N - n)$ - против. Мы можем утверждать, что вероятность p в этом случае оценивается величиной $\frac{n}{N}$.

Наша задача заключается в том, чтобы сказать, сколько измерений нужно проводить, чтобы быть уверенным, что p лежит в окрестности $(\frac{n}{N} - \delta p, \frac{n}{N} + \delta p)$ с вероятностью $1 - \alpha$, где α считается маленькой величиной.

Для простой оценки N мы можем вспомнить, что распределение величины n с данным значением p приближчнно подчиняется нормальному распределению

$$\frac{\frac{n}{N} - p}{\sqrt{\frac{p(1-p)}{N}}} \sim N(0, 1). \tag{21}$$

Так что мы можем оценить вероятность p быть в пределах интервала δp около значения $\frac{n}{N}$ как

$$P(\delta p, \sigma) = \frac{1}{\sqrt{2\pi}\sigma} \int\limits_{-\frac{\delta p}{2}}^{\frac{\delta p}{2}} e^{-\frac{x^2}{2\sigma^2}} dx, \tag{22}$$

где

$$\sigma = \sqrt{\frac{p(1-p)}{N}}. \tag{23}$$

Написав эту вероятность через α и, преобразовав интеграл, мы получим

$$1 - \alpha = 1 - \frac{2}{\sqrt{\pi}} \int\limits_{-\frac{\delta p}{2\sqrt{2}\sigma}}^{\infty} e^{-u^2} du, \tag{24}$$

в этом случае

$$\alpha = \frac{2}{\sqrt{\pi}} \int\limits_{\frac{\delta p}{2\sqrt{2}\sigma}}^{\infty} e^{-u^2} du. \tag{25}$$

Полагая α малым оценим интеграл (25) как

$$\int\limits_{x}^{\infty} e^{-u^2} du \sim \frac{e^{-x^2}}{x}. \tag{26}$$

Итак

$$\alpha \sim \frac{2}{\sqrt{\pi}} \frac{e^{-u^2}}{u}, \tag{27}$$

где

$$u = \frac{\delta p}{2\sqrt{2}\sigma} = \frac{\delta p \sqrt{N}}{2\sqrt{2p(1-p)}}. \tag{28}$$

Можно разрешить (28) как

$$u \sim \sqrt{\ln \frac{1}{\frac{\sqrt{\pi}}{2}\alpha \sqrt{\ln \frac{1}{\frac{\sqrt{\pi}}{2}\alpha}}}}, \tag{29}$$

Окончательно мы получим оценку для числа измерений

$$N \sim C \frac{p(1-p)}{\delta p^2}, \tag{30}$$

где

$$C = 8 \ln \frac{1}{\frac{\sqrt{\pi}}{2}\alpha \sqrt{\ln \frac{1}{\frac{\sqrt{\pi}}{2}\alpha}}}. \tag{31}$$

Для определчнности можно считать, что $\alpha = 0.01$. Это предположение достаточно разумное, но в любом случае оно влияет лишь на $C \approx 32$. Согласно (30) и $p(1-p) \approx \frac{1}{4}$ можно получить число измерений, которое необходимо проделать Еве

$$N \approx \frac{8}{\delta p^2}. \tag{32}$$

3.3 Определение квадратов коэффициентов в случае K спинов

Очевидно, что мы можем определить состояние лишь с некоторой вероятностью. Мы хотим получить оценку числа измерений N, необходимых чтобы определить каждый $p_x = |C_x|^2$ с вероятностью

$$1 - \alpha \approx 1 \tag{33}$$

в доверительном интервале δp, и так же считаем, что

$$\delta p / p = \beta \ll 1. \tag{34}$$

Ранее в (30) и (31) было показано, что для биномиального распределения с вероятностью p чтобы удовлетворить необходимому требованию понадобиться провести N измерений

$$N \sim C\frac{p(1-p)}{\delta p^2}. \tag{35}$$

Для вероятностей p_x чтобы найти систему в состоянии $|x\rangle$ мы можем использовать оценку

$$p \approx 2^{-K}. \tag{36}$$

В этом случае, используя (34) и (36), для (35) мы можем записать выражение вида

$$N \sim C\beta^{-2}2^K. \tag{37}$$

Для реалистичной оценки $\alpha = 0.01$ мы получим

$$N \sim 32\beta^{-2}2^K. \tag{38}$$

Полезно заметить, что β определяет величину точности с которой мы хотим определить состояние. Взломщик выбирает эту величину опираясь на априорную информацию о используемом унитарном преобразовании.

Есть лишь одно узкое место в этих рассуждениях, оно получается из (36), тем самым мы предполагаем, что все состояния практически равновероятны. Ожидается, что при значительном нарушении (36) состояния не будут максимально запутанными.

3.4 Определение фаз коэффициентов в случае K спинов

Чтобы определить желаемые фазы мы должны провести измерения вдоль нескольких осей, достаточно двух, и удобно, чтобы они были ортогональны.

Итак мы имеем следующую задачу. Есть 2^K комплексных коэффициентов, они преобразуются в C_x and C_y когда мы выбираем другие оси Ox и Oy соответственно. Наша задача заключается в том, чтобы выразить коэффициенты вдоль новых осей через старые коэффициенты, и затем написать систему уравнений.

Преобразование коэффициентов можно записать при помощи матриц поворота

$$\psi_{1/2m} = \sum_{m'} D^{1/2}_{m'm}(\alpha,\beta,\gamma)\psi_{1/2m'}, \tag{39}$$

где

$$D^{1/2}_{m'm}(\alpha,\beta,\gamma) = e^{im'\gamma}d^{1/2}_{m'm}(\beta)e^{im\alpha}, \tag{40}$$

$$d^{1/2}_{m'm}(\beta) = \begin{pmatrix} \cos\beta/2 & \sin\beta/2 \\ -\sin\beta/2 & \cos\beta/2 \end{pmatrix}, \tag{41}$$

и α, β и γ - углы Эйлера, $m = \pm 1/2$.

Итак состояния каждого спина трансформируются как

$$|1\rangle = D_{1/21/2}|1\rangle' + D_{1/2-1/2}|0\rangle' \tag{42}$$

$$|0\rangle = D_{-1/21/2}|1\rangle' + D_{-1/2-1/2}|0\rangle'. \tag{43}$$

Подставляем (42) в (43) в каждый член (13) и собираем коэффициенты перед одинаковыми состояниями.

Пересчитав коэффициенты C_i^x, через C_i^z, и, измерив вероятности вдоль оси X, мы можем написать систему уравнений на C_i^z

$$\begin{cases} |C_0^z|^2 = p_0^z \\ * \\ |C_{2^K-1}^z|^2 = p_{2^K-1} \\ |C_0^x|^2 = p_0^x \\ * \\ |C_{2^K-1}^x|^2 = p_{2^K-1}^x \end{cases} \tag{44}$$

Как уже было написано ранее, нам необходимо лишь два направления, чтобы определить все C_x. В самом деле, измерения квадратов коэффициентов вдоль двух осей дают нам $2(2^K-1)$ независимых вероятностей. Мы должны определить $2*2^K$ действительных параметра, так что два из них остаются свободными, они задают не что иное, как общий комплексный коэффициент перед разложением по базисным состояниям а он, как известно может быть произвольным.

Итак, мы получили, что для определения запутанного состояния с некоторой точностью необходимо

$$N \sim C\beta^{-2}2^K. \tag{45}$$

измерений идентичных ему состояний, а так же необходимо решать систему (44), состоящую из 2^{2K} нелинейных уравнений. В них нелинейность возникает при параметризации комплексных чисел, каждого - двумя действительными. Решение этой системы займчт полиномиальные время и ресурсы в зависимости от 2^K, то есть экспоненциально от числа взятых спинов.

4 Возможность подбора унитарного преобразования.

Получив оценку (45) можно было бы удовлетвориться тем, что она получается экспоненциальной по числу спинов. Но необходимо так же учесть, что Ева может избрать другую стратегию. И в самом деле, зачем ей находить матрицу какого-то унитарного преобразования, с уччтом того, что его всч равно потом придчтся переводить в схему квантовых вентилей, так может быть удобнее будет подбирать унитарное преобразование сразу в виде сети вентилей.

Ранее было уже замечено, что произвольное унитарное преобразование можно представить в виде сети квантовых вентилей, приччм для этого их понадобиться полиномиальное число от размерности матрицы преобразования, вообще говоря, зависимость квадратичная. Ясно, что это может быть громадное число, и даже Алисе и Бобу ни к чему будет использовать настолько сложные квантовые компьютеры. Поэтому понятно, что они будут использовать для своих целей гораздо меньшее число вентилей, пусть M штук. Нам необходимо понять, какое количество вариантов составления вычислительной сети придчтся перебрать Еве, чтобы отыскать правильную.

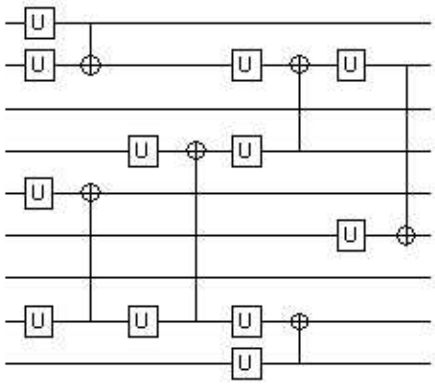

Рис. 1: Сеть венилей

Итак, пусть Ева подбирает схему из M двухспиновых элементов "исключающего или" , тогда число способов собрать из них схему будет оцениваться числом

$$N(K,M) = (K(K-1))^M, \tag{46}$$

это оценка сверху, так как в этой формуле не учитывается то, что собирая схему различными способами - подключая каждый последующий вентиль к выходам текущей схемы, мы на самом деле можем получать в точности одинаковые схемы. Но по существу зависимость должна остаться такой же.

Дальше необходимо учесть, что Алиса и Боб могут использовать различные односпиновые преобразования. Но эти преобразования могут быть различными, они даже могут зависеть от некоторого параметара. Перебрать континуальное множество элементов Ева никак не сможет, поэтому будем считать, что она выбирает некоторое количество L таких преобразований, так чтобы они как можно плотнее покрывали всч возможное пространство односпиновых преобразований. Тогда вместе с каждым вентилем "исключающего или" можно применять два односпиновых преобразования, например, до того, как применяем двухспиновое преобразование. Пример такой сети предложен на рис. 1. В этом случае полное число вариантов получится

$$N(K,L,M)a \approx K^{2M} * L^{2M}. \tag{47}$$

Как видно получается экспоненциальная зависимость от числа используемых вентилей. Эта формула, вообще говоря, ещч не учитывает того, что для каждой данной собранной сети вентилей необходимо проводить некоторое количество измерений запутанного состояния, чтобы убедиться в том, что верная схема действительно угадана.

Таким образом, мы приходим к выводу, что Алисе и Бобу в целях усиления безопасности необходимо не только увеличивать количество используемых спинов, но и усложнять используемую сеть вентилей.

5 Случай априорно известных временных корреляций.

5.1 Некоторые сведения из теории информации

Теперь мы переходим к рассмотрению более сложного случая, когда Еве известны лишь временные корреляции, под которыми мы будем понимать следующую величину

$$\xi_{kl}(i) = \langle p_k(x) p_l(x+i) \rangle_x, \tag{48}$$

где величина $p_k(x)$ равна единице, если x-ое слово это $|k\rangle$, и нулю в противном случае. Эта величина (48) называется временной корреляцией для слов $|k\rangle$ и $|l\rangle$.

Очевидно, что если два слова совсем никак не связаны, то и корреляции между ними никакой не будет. Довольно понятно, что методами архивирования информации можно уменьшать эти временные корреляции, что то же самое, что и смещение максимума корреляций в сторону больших времчн. Этот факт усложняет вскрытие шифра, поскольку проще всего воспользоваться коротковременными корреляциями.

Мы будем пользоваться следующим довольно очевидным фактом, что любое информационное сообщение должно содержать временные корреляции между словами, так как в противном случае это будет просто набор случайных слов. Напомним, что словом мы называем любую последовательность из K битов.

5.2 Случай одного спина

Допустим сначала для простоты, что Алиса посылает последовательность спинов с определчнными проекциями вдоль некоторой оси, приччм каждый спин задачт один бит информации. Мы считаем, что Ева не знает направления этой выбранной оси, и еч задача заключается в том, чтобы выяснить его. Соответственно единственное, чем она может пользоваться, это тем, что у передаваемых слов есть некоторые временные корреляции.

Чтобы предложить способ, при помощи которого можно определить это желаемое направление, заметим, что если измерять состояние спина вдоль оси перпендикулярной к выбранной, то никаких корреляций вообще не будет в силу законов квантовой механики, так как оба состояния спина будут проектироваться на эту ось с одинаковыми вероятностями. И, соответственно, при угле между осями не равными девяносто градусов, корреляции, если таковые были, останутся.

Таким образом нам надо найти направление таких двух осей, чтобы измерение спинов вдоль них не давало никаких временных корреляций. Тогда искомое направление секретной оси будет перпендикулярно обеим этим осям.

5.3 Случай K спинов

Здесь вся ситуация осложняется тем, что простыми поворотами оси мы не сможем задавать все возможные унитарные преобразования. Но всч же некоторые идеи можно развить из случая одного спина.

Заметим, что если спины не запутывать, то в случае K спинов тоже будет целая плоскость осей, измерения относительно которых будут давать абсолютно нескоррелированные результаты, - это все оси перпендикулярные оси Z, назовчм произвольную ось из это плоскости - осью X.

Но тогда можно рассуждать следующим образом: если бы Ева знала секретное преобразование U, то она могла бы подействовать им на состояния спинов с определчнными проекциями вдоль оси X, получить некоторые 2^K запутанных состояний, тогда утверждается, что проектируя состояния Алисы на эти состояния Ева будет получать абсолютно нескоррелированные результаты. По-другому можно обрисовать действия Евы таким образом: она применяет к запутанным состояниям Алисы "неизвестное ей" секретное обратное унитарное преобразование и проектирует эти состояния на ось X.

Тогда можно сформулировать задачу для Евы следующим образом. Она должна перебором получить такое унитарное преобразование спинов, что измерения относительно фиксированной оси не будут давать никаких временных корреляций. Это будет означать, что Ева нашла такое преобразование, которое, будучи применчнным к запутанным состояниям Алисы, получает некоторую перестановку исходных спинов, плюс некоторый случайный поворот на девяносто градусов для каждого спина в отдельности. Теперь ей остачтся лишь для каждого отдельно взятого спина найти по одному односпиновому преобразованию, которое как-то поворачивает этот спин, приччм временные корреляции всч ещч остаются нулевыми. Проделав такие манипуляции Ева получает для каждого спина два направления, которые задают перпендикулярное им искомое направление. Таким образом Ева получит унитарное преобразование, которое, будучи применчнным к запутанным состояниям Евы, будет давать состояния с определчнными значениями проекций вдоль оси Z, а это как раз означает, что Ева научится измерять каждое запутанное состояние ровно за один раз.

Обосновать предыдущий абзац можно следующим образом. Если мы после пробного преобразования Евы получаем наборы спинов, между которыми нет никаких корреляций, это и должно означать, что мы получили некоторое распутанное состояние спинов, а дальше остаются лишь односпиновые преобразования.

Теперь остачтся лишь оценить, сколько сообщений понадобиться перехватить Еве, чтобы найти это самое преобразование? Ответ на этот вопрос надо разделить на две части: во-первых, сколько необходимо использовать пробных унитарных преобразований, и, во-вторых, сколько различных измерений необходимо провести, чтобы понять, что временной коррелятор равен нулю. Здесь первая часть проблемы получается за сччт квантовой запутанности состояний, а вторая - в точности такая же, как и в случае классического шифра замены.

Необходимое количество различных пробных унитарных преобразований должно определяться размерностью матрицы преобразования, то есть порядка

$$N_{qu} \approx 2^{2K}, \tag{49}$$

это оценка сверху, здесь не учитывается, что необходимо подобрать преобразование с точностью до односпиновых преобразований. Можно конечно опять подбирать сеть из

вентилей, тогда согласно (47) получаем

$$N_{qu} \approx K^{2M} * L^{2M}. \tag{50}$$

Для решения классической части задачи необходимо учесть, что для измерения коррелятора необходимо будет измерить запутанные состояния полиномиальное число раз от числа 2^K

$$N_{cl} \approx P_n\left(2^K\right), \tag{51}$$

где степень n полинома $P_n(x)$ будет соответствовать учёту корреляций для всё больших времён.

Тогда по простой формуле

$$N_{net} \approx N_{qu} * N_{cl}. \tag{52}$$

Заключение

Итак мы получили, что в предложенном способе секретной передачи сообщений необходимое количество слов, которые необходимо перехватить Еве будет экспоненциально по числу используемых спинов и числу используемых квантовых вентилей, что определяется формулами (45) и (52).

Можно так же заметить, что согласно главе (5) основным преимуществом предложенной системы шифрования является то, что к обычным задачам классической криптографии добавляется так же проблема определения секретного унитарного преобразования. Основным источником такой дополнительной защиты является теорема о невозможности клонирования квантово-механической системы. Благодаря этой теореме измерение состояния спинов в неправильном базисе может принести гораздо меньше информации, чем в классическом случае, в котором единожды перехваченное сообщение может быть использовано для оценок временных корреляций в любой другой момент времени. Другими словами, перехватив в классическом случае некоторое количество сообщений, мы сразу же можем ими воспользоваться для расшифровки, в квантовом случае же часть из этих сообщений придётся безвозвратно потратить на то чтобы определить секретное унитарное преобразование.

Хотя идея шифрования информации запутанными состояниями довольно привлекательна, остаётться большое количество проблем при её реализации.

Во-первых, человечество до сих пор научилось манипулировать лишь единицами кубитов, что означает получение запутанных состояний лишь нескольких кубитов. И как это представляется на текущий момент, построение квантовых компьютеров - это дело ещё весьма отдалённого будущего.

Во-вторых, если запутанные состояния нескольких кубитов и удаётся создать, то это кубиты с системах реализованных на линейных ионных ловушках или ядерном магнитном резонансе. Однако необходимо ещё передать это запутанное состояние на некоторое расстояние. Времена декогентности в используемых системах настолько малы, что передача ионов или молекул с записанными на них кубитами будет возможна на очень маленькие расстояния. Пожалуй, единственным подходящим объектом для передачи запутанных состояний являются фотоны. Но к сожалению на данный момент

не существует способов переписывания состояния кубита в фотон и обратно с единичной вероятностью. Более того на данный момент напрямую удачтся создавать при помощи нелинейных оптических эффектов лишь пары запутанных фотонов [10].

Наконец, если даже проблема получения запутанных фотонов будет решена, то возникнет вопрос о дальности передачи. При передачах фотонов по какой либо среде неизбежно происходит влияние среды на состояния фотонов, например, направление их поляризации может испытывать отклонения от первоначального. Сейчас возможно передавать пару запутанных фотонов на расстояние порядка нескольких десятков километров по оптоволокну. Проблема в том, что, что не уменьшая секретности передачи, мы не можем усилить квантовый сигнал, поэтому на возможность связи на очень большие растояния возможна лишь в вакууме.

Список литературы

[1] R. Rivest, A. Shamir, L. Adleman, *On Digital Signatures and Public Key Cryptosystems*, MIT Laboratory for Computer Science, Technical Report, MIT/LCS/TR-212 (January 1979)

[2] R. Feynman, Int. J. Theor. Thys. **21**, 467, (1982)

[3] S.I.A.M. Journal on Computing, **26** (1997), 1484 and it is also available at quant-ph/9508027

[4] T. Cover and J. Thomas, *Elements of Information Theory*, John Wiley and Sons (1991)

[5] C. H. Bennet and G. Brassard, *Proc. IEEE Int. Conference on Computer Systems and Signal Processing*, IEEE, New York, (1984)

[6] A. Muller, J.Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993)

[7] W.K. Wooters and W.H. Zurek, Nature (London), **299**, 802, (1982)

[8] J.F. Clauser, M.A. Horne, A. Shimony, and R.A. Holt, Phys. Rev. Lett.**23**, 880 (1969)

[9] A. Ekert and R. Jozsa, Rev. Mod. Phys. **68**, 733 (1996)

[10] Y.H. Kim, M.V. Chekhova, S.P. Kulic, M.H. Rubin, and Y. Shin, Phys, Rev. A, **63**, 062301, (2001); J.D. Franson, Phys. Rev. Lett.,**62**, 2205, (1989)